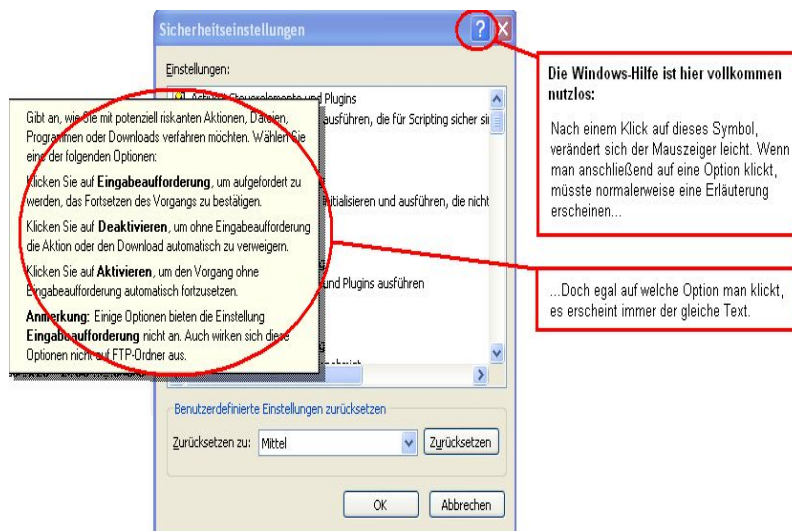


Die Sicherheit im Griff

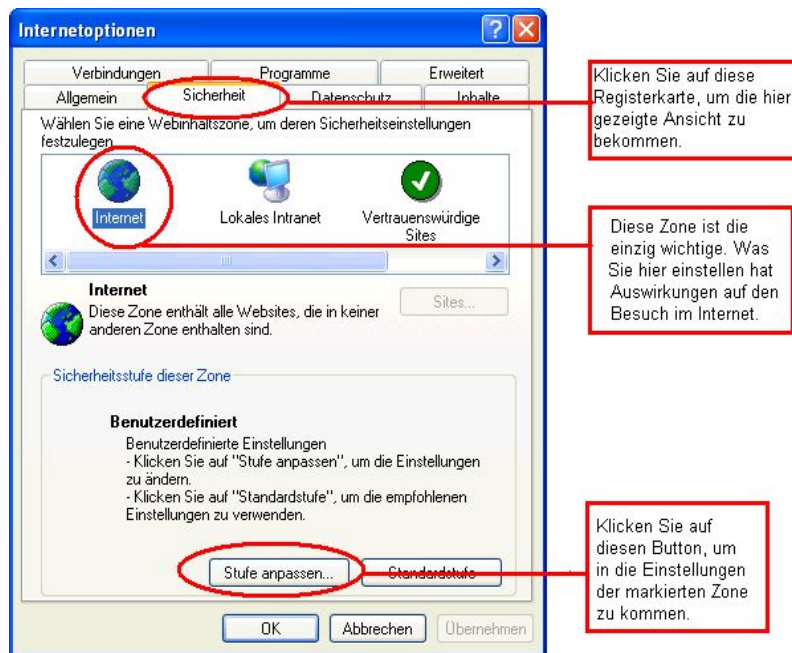
Vollständige Anleitungen sind im Internet nur schwer oder gar nicht zu finden und die Microsoft-Hilfe ist schlicht mangelhaft. So liefert die Stichwortsuche nicht einen einzigen Eintrag für grundlegende Begriffe, wie "Update", "Scripting" oder "Java". Wer sich im Menü für die Sicherheitseinstellungen befindet, kann von dort aus die Windows-Hilfe gar nicht aufrufen. Lediglich eine Kurzhilfe wird angeboten und die liefert bei allen aufgelisteten Funktionen einen immer gleichen Standardtext.



Bei den großen Sicherheitsproblemen, die der Internet Explorer hat, ist ein Verzicht auf die Erläuterungen der wichtigsten Optionen ein ganz böser Fehler. Vor allem, wenn sie so zahlreich und unübersichtlich sind: 31 Optionen erwarten den nichts ahnenden Nutzer, wenn er sich nur in die Sicherheitseinstellungen wagt. Der Großteil ist alles andere als selbst erklärend. Wer den Durchblick kriegen will, sollte jetzt Weiterlesen.

So kommt man in die Einstellungen

Im Internet Explorer kommt man über "Extras" >> "Internetoptionen" in die Einstellungen des Browsers. Dort schaltet man sich, mit einem Klick auf die verschiedenen Registerkarten am oberen Fensterrand, durch die einzelnen Menüs.



Wechsel Sie auf die Registerkarte "Sicherheit". Sie sehen jetzt in der oberen Hälfte des Fensters eine Reihe von Symbolen. "Internet", "Lokales Intranet", "Vertrauenswürdige Sites" und "Eingeschränkte Sites" sind die so genannten Zonen, die sich Microsoft für seinen Browser ausgedacht hat.

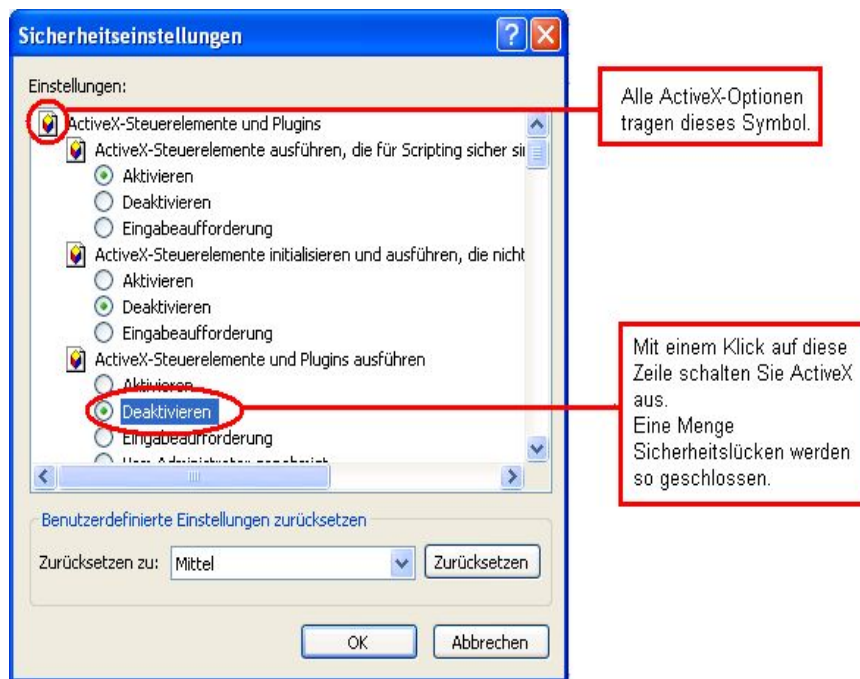
"Internet" ist die Zone, die Sie einstellen müssen. Die Sicherheitseinstellungen für die anderen drei kommen normalerweise nicht zur Anwendung. Denn Sie müssen seriöse und unseriöse Internetseiten zuvor in eigene Listen des Internet Explorers eingetragen haben, damit die letzten beiden Zonen überhaupt benutzt werden.

Außerdem muss Ihr Computer sich in einem Netzwerk mit eigenem Webseitenangebot befinden, damit die Einstellungen für "Lokales Intranet" zum Einsatz kommen. Dort sind die Sicherheitseinstellungen stark gelockert, weil in einem Intranet keine betrügerischen Internetseiten mit Viren und Spyware zu erwarten sind.

Einstellungen sind hier also Überflüssig. Für den normalen Gebrauch im Internet wählen Sie also das erste Symbol an und klicken auf "Stufe anpassen...", um jetzt die Einstellungen vorzunehmen. Sie sehen jetzt die wichtigsten Einstellungen des Browsers. 31 an der Zahl, mit unverständlichen Bezeichnungen und ohne Erläuterungen.

Sicherheitseinstellungen - die gruseligen 31

ActiveX-Einstellungen befinden sich ganz oben in der Liste. Die wichtigste Option befindet sich dabei an dritter Stelle. "ActiveX-Steuerelemente und Plugins ausführen" schaltet ActiveX an oder aus. Die anderen ActiveX-Einstellungen sind also wirkungslos, wenn diese Option auf "Deaktivieren" gesetzt wurde.



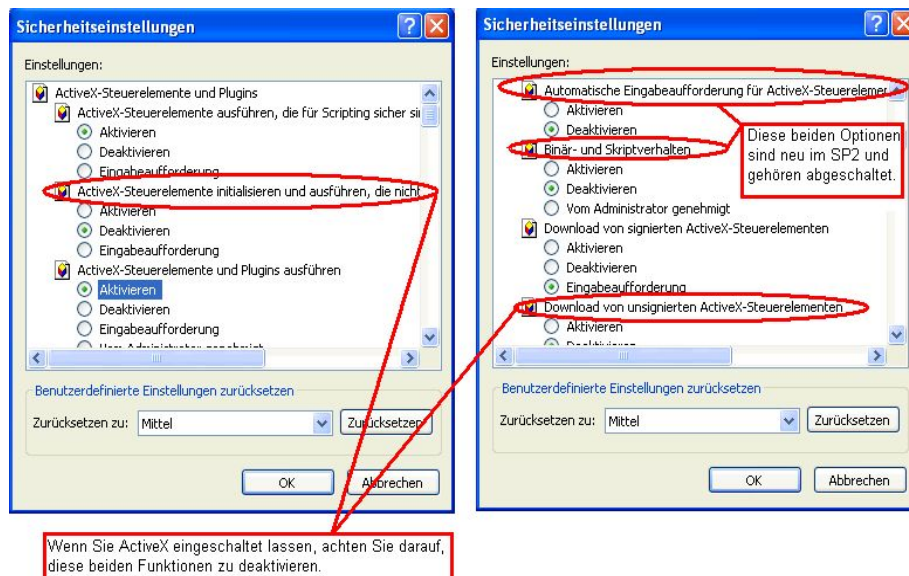
ActiveX ist eine kleine Programmiersprache, mit der Webseitenanbieter Ihre Seite aufpeppen können. Dummerweise kann man mit ActiveX auch auf Dateien zugreifen, sie verschieben oder sogar löschen. Diese Funktionen wurden schon oft missbraucht, um Computer zu schädigen. Es ist am sichersten, ActiveX abzuschalten.

Internetseiten, die ActiveX benutzen, funktionieren dann natürlich nicht mehr einwandfrei. Allerdings gibt es gar nicht so viele, die davon Gebrauch machen. Sie können also ruhig auf ActiveX verzichten. Zu den wenigen Internetseiten, die ActiveX benötigen, gehören die [Updateseite des Internet Explorers](#), die [Downloadseite von Macromedias Flash-Player](#) und einige Online-Virens Scanner.

ActiveX ist nicht so wichtig

Teilweise sind solche Seiten aber darauf ausgelegt, auch ohne ActiveX auszukommen. So erkennt etwa die Homepage von Macromedia automatisch, wenn kein ActiveX benutzt werden kann und leitet die Besucher dann zu einer Alternativseite um. Der Flash-Player kann dort durch einen gewöhnlichen Download-Link bezogen werden.

Wer auf seinem Computer einen Alternativbrowser ohne ActiveX installiert hat (wie etwa Firefox) kann den Internet Explorer dazu benutzen wollen, nur ActiveX-Seiten anzuschauen. In diesem Fall lässt man die Option natürlich auf "aktivieren" stehen oder wählt "Eingabeaufforderung". Mit letzterer Funktion erscheint vor dem Ausführen eines ActiveX-Angebots eine Abfrage. Sie können dann auswählen, ob ActiveX in diesem Moment benutzt werden darf oder nicht.



Wenn Sie ActiveX eingeschaltet lassen, sollten Sie aber unbedingt bei "ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind" und "Download von unsignierten ActiveX-Steuerelementen" auf "Deaktivieren" klicken. Außerdem gibt es durch das Service Pack 2 die neue Option "Automatische Eingabeaufforderung für ActiveX-Steuerelemente".

Hier sollten Sie "Deaktivieren" anwählen. Dadurch erscheint vor einer Softwareinstallation durch eine ActiveX-Seite (etwa von Macromedia Shockwave) eine Leiste mit einer Meldung am oberen Bildschirmrand. Erst wenn Sie auf diese Meldung klicken, wird die Installation gestartet. Normalerweise würde vorher nicht nachgefragt und die Software direkt installiert. Heimliche Installationen könnten so gestartet werden.

Mysteriöse neue Option ist wichtig

Die Optionen "ActiveX-Steuerelemente ausführen, die für Scripting sicher sind" und "Download von signierten ActiveX-Steuerelementen" setzen Sie am Besten auf "Eingabeaufforderung". So werden auch die etwas sichereren ActiveX-Angebote nicht ohne Nachfragen ausgeführt.

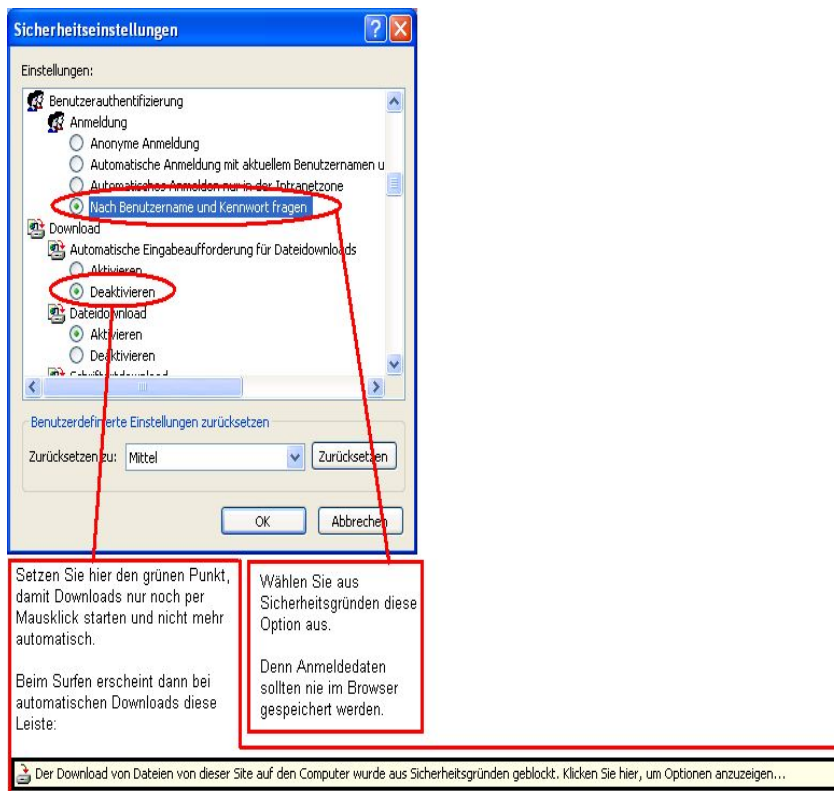
Die Option "Binär- und Skriptverhalten" ist durch das Service Pack 2 neu hinzugekommen. Microsoft widmet der neuen Funktion zwar [einen eigenen Beitrag auf seiner Internetseite](#), vergisst aber zu erklären, wofür die Option überhaupt gut ist. Lediglich eine Anleitung zum Abschalten wird dort geboten.

Virus überträgt sich durch Scrollen

Das ist tatsächlich auch angebracht. Denn in Testversuchen der amerikanischen Organisation "Bugtraq" konnte ein Virus programmiert werden, der sich mit Hilfe des Binärverhaltens überträgt. Sie brauchen lediglich auf einer präparierten Internetseite nach unten zu scrollen, um einen geheimen und schädlichen Download zu starten. Außerdem ist es möglich, die neue Datei dann automatisch bei jedem Windowsstart ausführen zu lassen.

Deshalb klicken Sie bei "Binär- und Skriptverhalten" natürlich auf "Deaktivieren". Zusätzlich empfiehlt es sich das [entsprechende Update von Microsoft](#) einzuspielen. Denn es gibt Schilderungen von Nutzern, bei denen sich der Testvirus übertragen konnte, obwohl die

Option abgeschaltet war. Wer kein SP2 auf dem Computer hat und somit auch nicht die neue Option zum Abschalten, sollte sich das Update ohnehin runterladen.



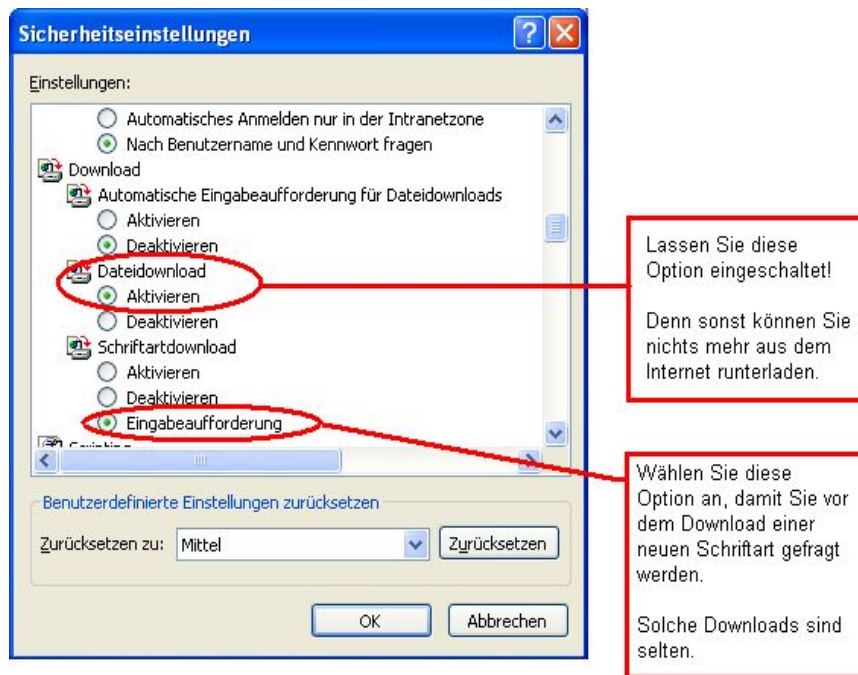
Die Option "Benutzerauthentifizierung" sollten Sie auf "Nach Benutzername und Kennwort fragen" setzen. Denn wenn Sie sich auf einer Internetseite anmelden, sollten Sie prinzipiell Name und Passwort selbst eintippen. Automatische Vorgänge sind an dieser Stelle immer unsicher, weil man die Anmeldedaten leichter ausspähen könnte.

Keine ungefragten Downloads

Die Rubrik "Download" hält drei Unteroptionen bereit. Die erste, "Automatische Eingabeaufforderung für Dateidownloads" sollten Sie auf "Deaktivieren" setzen. Dadurch werden Downloads nicht mehr automatisch gestartet, sondern erst durch Klick auf einen Link. Außerdem wird am oberen Rand der angezeigten Internetseite eine Zeile eingeblendet, wenn ein automatischer Download geblockt wurde.

Die zweite Option "Dateidownload" sollte aktiviert bleiben, schließlich wollen Sie ja noch Dateien aus dem Internet herunterladen können. Der Schriftartendownload gehört auf "Eingabeaufforderung" gesetzt, weil äußerst selten neue Schriftarten übertragen werden. Webseitengestalter achten darauf, dass nur die Schriftarten benutzt werden, die auf allen Computern zu Verfügung stehen.

Steht eine neue Schriftart zum Download an, ist das eine Ausnahme und sollte von Ihnen beabsichtigt sein. Mit der vorgenommenen Einstellung bittet der Explorer Sie, vor dem Download einer neuen Schriftart, um Bestätigung.



Java und JavaScript

Die beiden Skriptsprachen werden von vielen Internetseiten gebraucht und bieten Webseitengestaltern die Möglichkeit, kleine Programme zu schreiben. Im Unterschied zu richtigen Programmiersprachen sind sie aber nicht selbst lauffähig, sondern brauchen den Browser, um ausgeführt zu werden.

Durch die Möglichkeit der Programmierung, können natürlich auch schädliche Programme geschrieben werden, was den Browser unsicher macht. Denn ohne Skriptsprachen dient er lediglich der Anzeige von einfach gestalteten Internetseiten. Doch weil viele Internetangebote schöner designt werden können, wenn eine Skriptsprache im Spiel ist, kommt ein großer Teil der Internetseiten nicht ohne aus.